IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

M. ANDREW STOVER, *on behalf of himself and all others similarly situated*, Plaintiff, v. AT&T, INC., Defendant.	Case No. 3:24-cv-00863 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

M. Andrew Stover ("Plaintiff") brings this Class Action Complaint against AT&T, Inc. ("Defendant" or "AT&T"), on behalf of himself and all others similarly situated ("Class Members"), and alleges, upon personal knowledge as to his own actions and his counsel's investigations, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard personally identifiable information ("PII" or "Private Information")[1] including, but

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

not limited to full names, email addresses, mailing addresses, phone numbers, social security numbers, dates of birth, AT&T account numbers and passcodes.[2]

2. Defendant is headquartered and has its principal place of business at the corner of Akard and Commerce Street in Dallas, Texas two blocks from the Federal Courthouse. Defendant is an international telecommunications company that provides more than 100 million U.S. consumers with communications experiences across mobile and broadband.

3. To provide these services, and in the ordinary course of AT&T's business, Defendant acquires, possesses, analyzes, and otherwise utilizes Plaintiff's and Class Members' PII.

4. With this action, Plaintiff seeks to hold Defendant responsible for the harms it caused and will continue to cause Plaintiff and at least 7.6 million current customers and 65.4 million former account holders have been impacted[3] other similarly situated persons in the massive and preventable cyberattack purportedly discovered by Defendant, by which cybercriminals infiltrated Defendant's inadequately protected network servers and accessed and exfiltrated highly sensitive PII belonging to Plaintiff and Class Members which was being kept unprotected (the "Data Breach").

5. Plaintiff further seeks to hold Defendant responsible for its negligence in not ensuring that Defendant maintained the PII in a manner consistent with industry standards.

---

[2] Per the notice by email to Plaintiff at 9:08am C.S.T. on Easter Sunday morning (March 31, 2024) called an "update".

[3] See https://www.att.com/support/article/my-account/000101995?bypasscache=1 (last visited March 31, 2024).

6. Upon information and belief on or about March 30, 2024, AT&T began informing many Class Members that their sensitive PII had been compromised. It was called an "important update" although the Plaintiff's Easter morning email was the first notice received from AT&T about the data breach.

7. AT&T confirmed that Class Members' PII was released on the Dark Web.[4]

8. Upon information and belief, the Data Breach occurred in 2019 but Defendant did not begin informing victims of the Data Breach until March 30, 2024, approximately five years later. Indeed, Plaintiff and Class Members were wholly unaware of the Data Breach until they received Notice from Defendant. During this time, Plaintiff and Class Members were unaware that their sensitive PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. Plaintiff asserts this delay is outrageous.

9. The Notice provides no further information regarding the Data Breach and only recommends that victims reset their passwords, monitor their account activity, and potentially place fraud alerts on their account. The Notice does not explain how the Data Breach occurred, what steps Defendant took following the Data Breach, whether Defendant made any changes to its data security, or whether Plaintiff's and Class Members' PII remains in the possession of criminals.

10. By acquiring, utilizing, and benefiting from Plaintiff's and Class Members' PII for its business purposes, Defendant owed or otherwise assumed common law, contractual, and statutory duties that extended to Plaintiff and Class Members. These duties required Defendant to design and implement adequate data security systems to protect Plaintiff's and Class Members'

[4] *Id.*

PII in its possession and to keep Plaintiff's and Class Members' PII confidential, safe, secure, and protected from unauthorized disclosure, access, dissemination, or theft.

11. Defendant breached these duties by failing to implement adequate data security measures and protocols to properly safeguard and protect Plaintiff's and Class Members' PII from a foreseeable cyberattack on its systems that resulted in the unauthorized access and theft of Plaintiff's and Class Members' PII.

12. Currently, the full extent of the types of PII, the scope of the breach, and the root cause of the Data Breach are all within the exclusive control of Defendant, its agents, counsel, and forensic security vendors at this phase of the litigation.

13. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the Plaintiff's and Class Members' PII was compromised through disclosure to an unknown and unauthorized criminal third party.

14. Upon information and belief, Defendant breached its duties and obligations in one or more of the following ways: (1) failing to design, implement, monitor, and maintain reasonable network safeguards against foreseeable threats; (2) failing to design, implement, and maintain reasonable data retention policies; (3) failing to adequately train staff on data security; (4) failing to comply with industry-standard data security practices; (5) failing to warn Plaintiff and Class Members of Defendant's inadequate data security practices; (6) failing to encrypt or adequately encrypt the PII; (7) failing to recognize or detect that its network had been compromised and

accessed in a timely manner to mitigate the harm; (8) failing to utilize widely available software able to detect and prevent this type of attack, and (9) otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

15. Based on the type of sophisticated and targeted criminal activity, the type of PII involved, and Defendant's admission that the PII was accessed, it can be concluded that the unauthorized criminal third party was able to successfully target Plaintiff's and Class Members' PII, infiltrate and gain access to Defendant's network, and exfiltrate Plaintiff's and Class Members' PII, including full name, email address, mailing address, phone number, social security number, date of birth, AT&T account number and passcode, for the purposes of utilizing or selling the PII for use in future fraud and identity theft related cases. Upon information and belief they may have had as long as *five* (5) years to do so.

16. As a result of Defendant's failures and the Data Breach, Plaintiff's and Class Members' identities are now at a current and substantial imminent and ongoing risk of identity theft and shall remain at risk for the rest of their lives.

17. As Defendant instructed, advised, and warned in its Notice Letter discussed below, Plaintiff and Class Members must now closely monitor their financial accounts to guard against future identity theft and fraud. Plaintiff and Class Members have heeded such warnings to mitigate against the imminent risk of future identity theft and financial loss. Such mitigation efforts included and will include into the future: (a) reviewing financial statements; (b) changing passwords; and (c) signing up for credit and identity theft monitoring services. The loss of time and other mitigation costs are tied directly to guarding against and mitigating against the imminent risk of identity theft.

18. Plaintiff and Class Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) financial costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (e) loss of time heeding Defendant's warnings and following its instructions in the Notice Letter; (g) deprivation of value of their PII; (h) invasions of their privacy; and (i) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect it.

19. Plaintiff brings this action on behalf of all persons whose PII was compromised due to Defendant's failure to adequately protect Plaintiff's and Class Members' PII.

PARTIES

20. Plaintiff M. Andrew Stover is an adult individual and, at all relevant times herein, a resident and citizen of the state of Texas. Numerous class members are citizens of various states other than Texas.

21. Defendant AT&T, Inc. is a Texas corporation with its principal place of business at 208 South Akard Street, Dallas, Texas. Defendant is a citizen of Texas. AT&T's registered agent is CT Corporation System, 1999 Bryan ST., Ste. 900, Dallas, Texas 75201.

JURISDICTION AND VENUE

22. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant. It is known

that class members reside in Ohio, Georgia, Louisiana, Arizona, Oklahoma, and Missouri, as well as in other states.

23. This Court has general personal jurisdiction over Defendant AT&T because Defendant's principal place of business is in the Dallas Division of the Northern District of Texas and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District. The Defendant is a citizen of Texas.

24. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in the Dallas Division of the Northern District of Texas. In fact, AT&T's headquarters and principal place of business is two blocks from the Federal Courthouse in Dallas.

FACTUAL ALLEGATIONS

Background

25. Defendant AT&T is an international telecommunications corporation headquartered in Dallas, Texas. AT&T offers mobile communication services and broadband connectivity to millions of residential and business customers.

26. Defendant's Privacy Policy, posted on its website, states that AT&T "We work hard to safeguard your information using technology controls and organizational controls. We protect our computer storage and network equipment. We require employees to authenticate themselves to access sensitive data. We limit access to personal information to the people who need access for their jobs. And we require callers and online users to authenticate themselves before we provide account information.[5]

[5] *Privacy Policy*, https://about.att.com/privacy/privacy-notice.html (last visited Mar 31, 2024).

27. Defendant Privacy Policy also indicates that, "If a breach occurs, we'll notify you as required by law."[6]

28. Defendant's Notice Letter states, "We (AT&T) take cybersecurity very seriously and privacy is a fundamental commitment at AT&T."[7]

29. Indeed, Defendant has made numerous misleading representations that it would adequately protect Plaintiff's and Class Members' sensitive PII, but has failed to do so.

Defendant Acquires, Collects, and Stores the PII of Plaintiff and Class Members

30. In the ordinary course of its business, AT&T maintains the PII of its customers, current and past employees, consumers, and others.

31. Because of the highly sensitive and personal nature of the information Defendant acquires and stores with respect to consumers, Defendant, upon information and belief, promises to, among other things: keep protected information private; comply with insurance industry standards related to data security and PII, inform consumers of its legal duties and comply with all federal and state laws protecting consumer PII; only use and release PII for reasons that relate to medical care and treatment, and, provide adequate notice to individuals if their PII is disclosed without authorization.

32. At every step, Defendant holds onto sensitive PII and has a duty to protect that PII from unauthorized access.

33. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that

[6] *Id.*

[7] See *Notice Letter*.

it was responsible for protecting Plaintiff's and Class Members' PII from unauthorized disclosure.

34. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

35. Plaintiff and Class Members relied on Defendant to implement and follow adequate data security policies and protocols, to keep their PII confidential and securely maintained, to use their PII solely for proper business services and purposes, and to prevent the unauthorized disclosure of their PII.

The Cyberattack and Data Breach

36. AT&T detected unauthorized access to certain computer systems within its network environment.[8]

37. AT&T reset passcodes for AT&T accounts.[9]

38. Through its investigation, AT&T determined that the data of 7.6 million current AT&T account holders and 65.4 million former account holders.[10]

39. Upon information and belief, Plaintiff's and Class Members' PII was exfiltrated and stolen in the attack.

40. Furthermore, the investigation determined that the accessed systems contained PII. Upon information and belief, this PII was accessible, unencrypted, unprotected, and vulnerable to acquisition and/or exfiltration by the unauthorized actor.

41. The type of PII accessed by the unauthorized actor in the Data Breach includes full

[8] *See https://www.att.com/support/article/my-account/000101995?bypasscache=1 (last visited March 31, 2024).*

[9] *Id.*

[10] *Id.*

name, email address, mailing address, phone number, social security number, date of birth, AT&T account number and passcode.[11]

42. While AT&T stated in the Notice Letter that the unusual activity involved data sets from 2019, AT&T did not begin notifying victims until March 30, 2024 after AT&T discovered that the PII of Plaintiff and Class Members were posted on the Dark Web.[12]

43. Defendant had obligations created by contract, industry standards, common law, and its own promises and representations to keep Plaintiff's and Class Members' PII confidential and to protect it from unauthorized access and disclosure.

44. Plaintiff and Class Members provided their PII directly, or indirectly, to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

45. Through its Notice Letter, AT&T also recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to take steps to mitigate their risk of identity theft, such as reviewing financial accounts, and reviewing credit reports for possible fraud.

46. Beginning on or around March 30, 2024, Defendant issued Notice Letters by email and mail to Plaintiff and Class Members. In total, at least seventy-three million individuals were impacted by the Data Breach.[13]

[11] *Id.*

[12] *Id.*

[13] See *Id.*

47. The Notice Letters sent to Plaintiff and Class Members stated PII, including full names, email addresses, mailing addresses, phone numbers, social security numbers, dates of birth, AT&T account numbers and passcodes were accessed and exfiltrated in the Data Breach.

48. As a result of the Data Breach, Plaintiff and seventy-three million Class Members suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack and the substantial and imminent risk of identity theft.

49. Defendant waited approximately five years to disclose the Data Brach to Plaintiff and Class Members, and only did so after the PII belonging to Plaintiff and Class Members were posted by cyber criminals on the Dark Web. As a result of this delay, Plaintiff and Class Members had no idea their PII had been compromised in the Data Breach, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

50. Defendant's failure to timely detect and report the Data Breach, giving cyber criminals a five year head start, made its consumers vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

51. This PII was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the PII of Plaintiff and Class Members.

52. Despite recognizing its duty to do so, on information and belief, Defendant has not implemented reasonable cybersecurity safeguards or policies to protect its consumers' PII or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a

result, Defendant leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to consumers' PII.

53. Plaintiff and Class Members directly or indirectly entrusted Defendant with sensitive and confidential information, including their PII which includes information that is static, does not change, and can be used to commit myriad financial crimes.

54. Plaintiff and Class Members relied on Defendant to keep their PII confidential and securely maintained, to use their PII for authorized purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand Defendant safeguard their PII.

55. The unencrypted PII of Plaintiff and Class Members will likely end up for sale on the dark web as that is the *modus operandi* of hackers. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. In turn, unauthorized individuals can easily access the PII of Plaintiff and Class Members.

56. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiff and Class Members, causing the exposure of PII.

DefendantHad an Obligation to Protect the PII

57. Defendant's failure to adequately secure Plaintiff's and Class Members' PII breaches duties it owes Plaintiff and Class Members under statutory and common law. Moreover, Plaintiff and Class Members surrendered their highly sensitive personal data to Defendant under the implied condition that Defendant would keep it private and secure. Accordingly, Defendants also Has an implied duty to safeguard Its data, independent of any statute.

58. Defendant was prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. S*ee, e.g.*, *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

59. Therefore, the increase in such attacks, and the attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

60. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII of Plaintiff and Class Members.

61. Defendant owed a duty to Plaintiff and Class Members to design, maintain, and test its computer systems, servers, and networks to ensure that the PII in its possession was adequately secured and protected.

62. Defendant owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the PII in its possession, including not sharing information with other entities who maintained substandard data security systems.

63. Defendant owed a duty to Plaintiff and Class Members to implement processes that would immediately detect a breach on its data security systems in a timely manner.

64. Defendant owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

65. Defendant owed a duty to Plaintiff and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to entrust this PII to Defendant.

66. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

67. Defendant owed a duty to Plaintiff and Class Members to encrypt and/or more reliably encrypt Plaintiff's and Class Members' PII and monitor user behavior and activity in order to identify possible threats.

68. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members and the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

69. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to, at least, tens of thousands of individuals' PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

Defendant Failed to Properly Protect Plaintiff's and Class Members' PII

70. Defendant could have prevented this Data Breach by properly securing and encrypting the systems containing the PII of Plaintiff and Class Members. Alternatively,

Defendant could have destroyed the data, especially for individuals with whom it had not had a relationship for a period of time.

71. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to companies like Defendant to protect and secure sensitive data they possess.

72. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

73. As a result of computer systems in need of security upgrades, inadequate procedures for handling email phishing attacks, viruses, malignant computer code, hacking attacks, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII.

74. Because Defendant failed to properly protect and safeguard Plaintiff's and Class Members' PII, an unauthorized third party was able to access Defendant's network, and access Defendant's database and system configuration files and exfiltrate that data.

Defendants Failed to Comply with Industry Standards

75. Experts studying cyber security routinely identify companies in the Telecommunications industry as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

76. Several best practices have been identified that at a minimum should be implemented by Telecommunications service providers like Defendant, including, but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

77. Other best cybersecurity practices that are standard in the Telecommunications industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

78. Upon information and belief, Defendant failed to comply with one or more industry standards.

Defendant's Negligent Acts and Breaches

79. Defendant participated in and controlled the process of gathering the PII from Plaintiff and Class Members.

80. Defendant therefore assumed and otherwise owed duties and obligations to Plaintiff and Class Members to take reasonable measures to protect the information, including the duty of oversight, training, instruction, testing of the data security policies and network systems. Defendant breached these obligations to Plaintiff and Class Members and/or was otherwise negligent because it failed to properly implement data security systems and policies for its Telecommunications services network that would adequately safeguard Plaintiff's and Class Members' PII. Upon information and belief, Defendant's unlawful conduct included, but is not limited to, one or more of the following acts and/or omissions:

a. Failing to design and maintain an adequate data security system to reduce the risk of data breaches and protect Plaintiff's and Class Members' PII;

b. Failing to properly monitor its data security systems for data security vulnerabilities and risk;

c. Failing to test and assess the adequacy of its data security system;

d. Failing to develop adequate training programs related to the proper handling of emails and email security practices;

e. Failing to develop and put into place uniform procedures and data security protections for its network;

f. Failing to adequately fund and allocate resources for the adequate design, operation, maintenance, and updating necessary to meet industry standards for data security protection;

g. Failing to ensure or otherwise require that it was compliant with FTC guidelines for cybersecurity;

h. Failing to ensure or otherwise require that it was adhering to one or more of industry standards for cybersecurity discussed above;

i. Failing to implement or update antivirus and malware protection software in need of security updating;

j. Failing to require encryption or adequate encryption on its data systems;

k. Otherwise negligently and unlawfully failing to safeguard Plaintiff's and Class Members' PII provided to Defendant, which in turn allowed cyberthieves to access its IT systems.

COMMON INJURIES & DAMAGES

81. As result of Defendant's ineffective and inadequate data security practices, Plaintiff and Class Members now face a present and ongoing risk of fraud and identity theft.

82. Due to the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) loss of time due to increased spam and targeted marketing emails; (e) the loss of benefit of the bargain (price premium

damages); (f) diminution or loss of value of their PII; and (g) the continued risk to their PII, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

83. Defendant's failure to properly notify Plaintiff and Class Members of the Data Breach in a timely fashion exacerbated Plaintiff's and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Loss of Time to Mitigate the Risk of Identify Theft and Fraud

84. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

85. Thus, due to Defendant's admitted recognition of the actual and imminent risk of identity theft, Defendant has encouraged customers to remain vigilant by monitoring account activity and credit reports and to set up free fraud alerts with Equifax, Experian, and TransUnion. The plaintiff did that, taking uncompensated personal time to do so.

86. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and

filing police reports, which may take years to discover and detect.

87. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[14]

88. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[15]

89. The FTC recommends that identity theft victims take several steps and spend time to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[16]

---

[14] *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-07-737, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN (2007) ("GAO Report"), available at https://www.gao.gov/new.items/d07737.pdf (last visited March 31, 2024).

[15] *See* Federal Trade Commission, IdentityTheft.gov, https://www.identitytheft.gov/Steps (last visited March 31, 2024).

[16] *See* Federal Trade Commission, IdentityTheft.gov, https://www.identitytheft.gov/Steps (last visited March 31, 2024).

Diminution of Value of the PII

90. PII is a valuable property right.[17] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

91. For example, drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves.

92. PII can sell for as much as $363 per record according to the Infosec Institute.[18]

93. Medical information is especially valuable to identity thieves. Cybersecurity firm Trustwave calculated the black-market value of medical records at $250 each.[19]

94. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[20] In fact, the data marketplace is so

---

[17] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[18] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited March 31, 2024).

[19] Paul Ndrag, *Medical records are the hottest items on the dark web*, Fierce Healthcare (Jan. 26, 2021), https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web (last visited March 31, 2024).

[20] David Lazarus, *Column: Shadowy data brokers make the most of their invisibility cloak*, LA Times (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited March 31, 2024).

sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[21, 22] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[23]

95. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished in its value by its unauthorized and potential release onto the Dark Web, where it may soon be available and holds significant value for the threat actors.

Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary

96. To date, Defendant has done nothing to provide Plaintiff and Class Members with relief for the damages they have suffered as a result of the Data Breach.

97. Defendant only encourages Plaintiff and Class Members to remain vigilant by monitoring account activity and credit reports and to sign up for free fraud alerts from nationwide credit bureaus — Equifax, Experian, and TransUnion. Defendant also places the burden squarely on Plaintiff and Class Members by requiring them to independently sign up for that service.

98. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII, and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/Dark Web for sale and purchase by criminals intending to utilize the PII for identity theft crimes – e.g.,

[21] https://datacoup.com/.

[22] https://digi.me/what-is-digime/.

[23] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited March 31, 2024).

opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

99. It must be noted there may be a substantial time lag – measured in years – between when harm occurs versus when it is discovered, and also between when PII and/or financial information is stolen and when it is used.

100. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

101. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[24] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

102. Consequently, Plaintiff and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future.

103. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year, or more, per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future

[24] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1 (last visited March 31, 2024

cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their PII.

104. Moreover, Plaintiff and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing PII is not accessible online and that access to such data is password protected.

Plaintiff's M. Andrew Stover's Individual Experience

105. At the time of the Data Breach, Defendant retained Plaintiff Stover's PII in its system.

106. In order to obtain services from AT&T, Plaintiff Stover was required to provide his Private Information to AT&T.

107. Plaintiff Stover received an email notice on Easter Sunday morning at 9:08am C.S.T. on March 31, 2024, directly from AT&T. According to the Notice email, Plaintiff Stover's PII was improperly accessed and obtained by unauthorized third parties. It titled the email subject line "Important Update." This was totally misleading. You cannot "update" information you have never given to the Plaintiff.

108. As a result of the Data Breach, and at the direction of AT&T's Notice Letter, Plaintiff Stover made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to, spending his own uncompensated time monitoring his financial accounts, implementing extra security on his computers, changing all his passwords across all accounts and devices and contacting Experian, Equifax and Transunion to assure his credit accounts were frozen.. Plaintiff Stover has spent significant time dealing with the Data Breach, valuable time

Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This uncompensated time has been lost forever and cannot be recaptured, all as a result of AT&T's negligence.

109. Plaintiff Stover suffered actual injury from having his PII compromised as a result of the Data Breach, including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of his PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity cost associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in AT&T's possession and is subject to further unauthorized disclosures so long as AT&T fails to undertake appropriate and adequate measures to protect the PII.

110. After the Data Breach, Plaintiff Stover was informed that his PII might be available on the Dark Web.

111. The Data Breach has caused Plaintiff Stover to suffer fear, anxiety and stress, which has been compounded by the fact that AT&T has still not fully informed him of key details about the Data Breach's occurrence.

112. Plaintiff Stover anticipates spending considerable time on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

113. As a result of the Data Breach, Plaintiff Stover is at present risk and will continue to be at increased risk of identity theft and fraud for the rest of his life.

114. Plaintiff Stover has a continuing interest in ensuring that his PII which, on

information and belief, remains backed up in AT&T's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

115. Plaintiff brings this nationwide class action on behalf of himself and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

116. The nationwide class that Plaintiff seeks to represent is defined as follows:

> **All United States residents who were notified by email or standard mail that their PII was compromised in the AT&T Data Breach (the "Class").**

117. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

118. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

119. Numerosity, Fed R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are at least multiple thousands of individuals who were notified by Defendant of the Data Breach. According to Defendant's statement posted on its company website, at least seventy-three million current customers had their

PII compromised in this Data Breach.[25] The identities of Class Members are ascertainable through Defendant's records, Class Members' records, publication notice, self-identification, and other means.

120. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendant had duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had duties not to use the PII of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in

[25] See https://www.att.com/support/article/my-account/000101995?bypasscache=1 (last visited March 31, 2024).

the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members;

k. Whether Defendant violated the consumer protection statutes invoked herein;

l. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

m. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

n. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

121. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance.

122. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

123. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent

and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

124. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

125. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that

experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

126. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

127. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

128. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

129. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

130. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members;

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

131. Plaintiff re-alleges and incorporates by reference herein all of the allegations above.

132. Plaintiff and the Class entrusted Defendant with their PII.

133. Plaintiff and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business

purposes only, and/or not disclose their PII to unauthorized third parties.

134. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

135. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

136. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII of Plaintiff and the Class in Defendant's possession was adequately secured and protected.

137. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII it was no longer required to retain.

138. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiff and the Class.

139. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant, either directly or indirectly, with their confidential PII, a necessary part of obtaining services from Defendant.

140. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

141. A breach of security, unauthorized access, and resulting injury to Plaintiff and the

Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

142. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

143. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII of Plaintiff and the Class, including basic encryption techniques freely available to Defendant.

144. Plaintiff and the Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

145. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

146. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

147. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and the Class.

148. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost

and disclosed to unauthorized third persons as a result of the Data Breach.

149. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and the Class during the time the PII was within Defendant's possession or control.

150. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

151. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiff and the Class in the face of increased risk of theft.

152. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of PII.

153. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove PII that it was no longer required to retain pursuant to regulations.

154. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data Breach.

155. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the PII of Plaintiff and the Class would not have been compromised.

156. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The PII of Plaintiff and the Class was lost

and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

157. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

158. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

159. Defendant's violation of Section 5 of the FTC Act constitutes negligence.

160. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

161. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

162. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from

identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiff and the Class; and (viii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

163. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

164. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

165. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
Breach Of Implied Contract
(On behalf of Plaintiff and the Class)

166. Plaintiff re-alleges and incorporates by reference herein all of the allegations above.

167. The PII of Plaintiff and Class Members, including full names and Social Security numbers, was provided and entrusted to Defendant.

168. Plaintiff and Class Members provided their PII to Defendant, either directly or indirectly, through Defendant's clients, as part of Defendant's regular business practices.

169. Plaintiff and the Class entrusted their PII to Defendant. In doing so, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen. As a condition of obtaining services and being employed by Defendant's clients, Plaintiff and Class Members provided and entrusted their PII. In so doing, Plaintiff and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and Class Members if their data had been breached and compromised or stolen.

170. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide their PII to Defendant and/or Defendant's clients with the reasonable understanding that their PII would be adequately protected by any business associates, like Defendant, from foreseeable threats. This inherent understanding exists independent of any other law or contractual obligation any time that highly sensitive PII is exchanged as a condition of receiving services. It is common sense that but for this implicit and/or explicit agreement, Plaintiff and Class Members would not have provided their PII.

171. Defendant separately has contractual obligations arising from and/or supported by the consumer facing statements in its Privacy Policy.

172. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

173. Defendant breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect their PII and by failing to provide timely and accurate notice that PII was compromised as a result of the Data Breach.

174. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and Class Members have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

175. As a result of Defendant's breach of implied contract, Plaintiff and Class Members are entitled to and demand actual, consequential, and nominal damages.

COUNT III
Unjust Enrichment
(On behalf of Plaintiff and the Class)

176. Plaintiff re-alleges and incorporates by reference herein all of the allegations above. Notwithstanding, Plaintiff brings this claim in the alternative to any claim for breach of contractual obligations.

177. Defendant benefited from receiving Plaintiff's and Class Members' PII by its ability to retain and use that information for its own benefit. Defendant understood this benefit.

178. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII.

179. Defendant was also enriched from the value of Plaintiff's and Class Members' PII. PII has independent value as a form of intangible property. Defendant also derives value from this information because it allows Defendant to operate its business and generate revenue.

180. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

181. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

182. Defendant acquired the monetary benefit and PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

183. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

184. Plaintiff and Class Members have no adequate remedy at law.

185. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft;

(ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in their continued possession and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

186. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

187. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them.

COUNT IV
Breach Of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

188. Plaintiff re-alleges and incorporates by reference herein all of the allegations above.

189. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became guardian of Plaintiff's and Class Members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' PII; (2) to timely notify Plaintiff and Class Members of the Data Breach and disclosure; and (3) to maintain complete and

accurate records of what information (and where) Defendant did and does store.

190. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant's relationship with its customers, in particular, to keep secure their PII.

191. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

192. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to encrypt or otherwise protect the integrity of the systems containing Plaintiff's and Class Members' PII.

193. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

194. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' PII.

195. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as

Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

196. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and economic and non-economic losses.

COUNT IV
Breach of the Implied Covenant of Good Faith and Fair Dealing
(On Behalf of Plaintiff and the Class)

197. Plaintiff re-allege and incorporate by reference herein all of the allegations above.

198. Every contract in this state has an implied covenant of good faith and fair dealing. This implied covenant is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

199. Plaintiff and Class Members have complied with and performed all conditions of their contracts with Defendant.

200. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII, failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members and continued acceptance of PII and storage of other personal information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

201. Defendant acted in bad faith and/or with malicious motive in denying Plaintiff and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Classes, and appointing Plaintiff and his Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendant to delete, destroy, and purge the PII of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII

of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to

identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including, but not limited to, actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: April 8, 2024

Respectfully Submitted,

s/ Joe Kendall
JOE KENDALL
Texas Bar No. 11260700
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 825
Dallas, Texas 75219
Phone:214-744-3000
Fax: 214-744-3015
jkendall@kendalllawgroup.com

Counsel for Plaintiff and the Putative Class